

Accessible Information and Informational Power of Quantum 2-designs

Michele Dall'Arno^{1,*}

¹*Centre for Quantum Technologies, National University of Singapore,
3 Science Drive 2, 117543 Singapore, Republic of Singapore*

(Dated: November 13, 2014)

The accessible information and the informational power quantify the amount of information extractable from a quantum ensemble and by a quantum measurement, respectively. So-called spherical quantum 2-designs constitute a class of ensembles and measurements relevant in testing entropic uncertainty relations, quantum cryptography, and quantum tomography. We provide lower bounds on the entropy of 2-design ensembles and measurements, from which upper bounds on their accessible information and informational power follow, as a function of the dimension only. We show that the statistics generated by 2-designs, although optimal for the abovementioned protocols, never contains more than one bit of information. Finally, we specialize our results to the relevant cases of symmetric informationally complete (SIC) sets and maximal sets of mutually unbiased bases (MUBs), and we generalize them to the arbitrary-rank case.

I. INTRODUCTION

Quantum theory is arguably the most complete and successful description of the inherent evolution of physical systems. At the same time, any information we can access about physical systems is ultimately classical. The interface between the quantum and classical domains is constituted by quantum ensembles and quantum measurements, the former capable of preparing quantum states upon input of some classical information, the latter of extracting some classical information from quantum systems.

From the fundamental viewpoint, it is thus crucial to characterize ensembles and measurements in terms of the maximal amount of extractable information, leading to results such as entropic uncertainty relations [1–5] and device-independent quantum information processing [6]. This characterization has deep consequences in a plethora of applications, such as information locking [7], quantum cryptography [8], tomography [9], communication [10], witnessing [11, 12], private decoupling [13, 14], purification of noisy measurements [15], and error correction [16, 17], where the efficiency – or the success itself – of the protocol depends on the generated input-output statistics.

In this paper we address the problem of quantifying the maximal amount of information that can be extracted from a quantum ensemble, or by a quantum measurement. The former problem, known as the *accessible information problem*, was introduced [18–23] almost half a century ago, while the

latter, known as the *informational power problem*, is much younger [24–30].

We will focus on a relevant class of ensembles and measurements, known as spherical quantum 2-designs [31], whose distinctive feature is to share many properties with the uniform distribution. Relevant examples of 2-designs are so-called symmetric, informationally complete (SIC) measurements [32, 33], and maximal sets of mutually unbiased bases (MUBs) [34, 35]. They play a crucial role in our understanding of the state space [36, 37], in quantum Bayesianism [38–41], and are key ingredients in many of the abovementioned quantum information processing protocols.

We derive lower bounds on the entropy of the input distribution of 2-design ensembles and of the output distribution of 2-design measurements. From these results, we derive upper bounds on the accessible information and the informational power of 2-design ensembles and measurements, as a function of the dimension of the system only. As a consequence, we show that, perhaps surprisingly, the statistics generated by 2-designs, although optimal for the abovementioned protocols, never contains more than one bit of information. As particular cases, we provide the accessible information and informational power of SIC and MUB ensembles and POVMs (analytically for dimensions two and three, numerically otherwise). Finally, we extend our results to generalizations of SICs and MUBs with arbitrary rank.

The paper is structured as follows. Preliminary concepts are summarized in Sec. II. Lower bounds on the entropy of 2-designs are derived in Sec. III, from which bounds on accessible information and informational power of 2-designs are derived in Sec. IV.

* cqtmada@nus.edu.sg

Our results are specialized to the cases of SICs and MUBs in Sec. V, and generalized to the arbitrary-rank case in Sec. VI. We conclude the paper discussing some open problems in Sec. VII.

II. FORMALISM

Let us recall some basic facts [42] from quantum information theory. Any quantum system is associated with an Hilbert space \mathcal{H} , and we denote with $L(\mathcal{H})$ the space of linear operators on \mathcal{H} . We consider only finite dimensional Hilbert spaces. A *quantum state* ρ is a positive semidefinite operator in $L(\mathcal{H})$ such that $\text{Tr}[\rho] \leq 1$. Any preparation of a quantum system is described by an *ensemble*, namely an operator-valued measurable function $E = \{\rho_x\}$ from real numbers x to states $\rho_x \in L(\mathcal{H})$, such that $\sum_x \text{Tr}[\rho_x] = 1$.

A *quantum effect* Π is a positive semidefinite operator in $L(\mathcal{H})$ such that $\Pi \leq \mathbb{1}$. Any measurement on a quantum system is described by a *positive-operator valued measure* (POVM), namely an operator-valued measurable function $P = \{\Pi_y\}$ from real numbers y to effects $\Pi_y \in L(\mathcal{H})$, such that $\sum_y \Pi_y = \mathbb{1}$, where $\mathbb{1}$ denotes the identity operator. Given an ensemble $E = \{\rho_x\}$ and a POVM $P = \{\Pi_y\}$, the joint probability $p_{x,y}$ of state ρ_x and outcome Π_y is given by the Born rule, namely $p_{x,y} = \text{Tr}[\rho_x \Pi_y]$.

A. Accessible information and informational power

Let us recall some basic definitions [43] from classical information theory. A random variable X is a function that maps from its domain, the sample space, to its range, the real numbers, according to a probability distribution p_x . Given a random variable X , its *Shannon entropy* $H(X)$ defined as

$$H(X) := - \sum_x p_x \log p_x,$$

is a measure of the lack of information about the outcome of X . We write \log for binary logarithms and \ln for natural logarithms, and we express informational quantities in bits.

Given two random variables X and Y , their *joint Shannon entropy* $H(X, Y)$ is defined as

$$H(X, Y) := - \sum_{x,y} p_{x,y} \log p_{x,y},$$

is a measure of the lack of information about the joint outcomes of X and Y . The *conditional Shannon entropy* $H(Y|X)$ defined as $H(Y|X) := H(X, Y) - H(X)$ is a measure of the lack of information about the outcome of X given the knowledge of the outcome of Y . The *mutual information* $I(X; Y)$ defined as $I(X; Y) := H(X) + H(Y) - H(X, Y) = H(Y) - H(Y|X) = H(X) - H(X|Y)$ is a measure of how much information about each random variable is carried by the other one. Given an ensemble $E = \{\rho_x\}$ and a POVM $P = \{\Pi_y\}$, we denote with $I(E, P)$ the mutual information $I(X; Y)$ between random variables X and Y distributed according to $p_{x,y} = \text{Tr}[\rho_x \Pi_y]$.

The accessible information [18–21] is a measure of how much information can be extracted from an ensemble.

Definition 1 (Accessible information). *The accessible information $A(E)$ of an ensemble E is the supremum over any POVM P of the mutual information $I(E, P)$, namely*

$$A(E) := \sup_P I(E, P).$$

The informational power [24] is a measure of how much information can be extracted by a POVM.

Definition 2 (Informational power). *The informational power $W(P)$ of a POVM P is the supremum over any ensemble E of the mutual information $I(E, P)$, namely*

$$W(P) := \sup_E I(E, P).$$

We recall some results about accessible information and informational power that will be useful in the following.

Lemma 1. *For any POVM $P = \{\Pi_y\}$, the informational power $W(P)$ is the supremum over normalized states ρ of the accessible information of the ensemble $\{\rho^{1/2} \Pi_y \rho^{1/2}\}$, namely*

$$W(P) = \sup_{\rho} A(\{\rho^{1/2} \Pi_y \rho^{1/2}\}). \quad (1)$$

Proof. See Refs. [24, 29]. \square

Lemma 2. *For any ensemble E of pure states and for any POVM P with rank-one elements, the accessible information $A(E)$ and the informational power $W(P)$ are bounded as follows:*

$$0 \leq A(E) \leq \log d. \quad (2)$$

$$\log d - \frac{1}{\ln 2} \sum_{n=2}^d \frac{1}{n} \leq W(P) \leq \log d. \quad (3)$$

Proof. See Refs. [19, 23, 29]. \square

B. Spherical quantum 2-designs

A spherical quantum t -design is a discrete probability distribution over quantum states that shares some properties with the uniform distribution.

Definition 3 (Spherical quantum t -design). *A spherical quantum t -design $\{p_x, |\phi_x\rangle\}_{x=1}^N$ is a probability distribution p_x over normalized pure states $|\phi_x\rangle$ such that*

$$\sum_{x=1}^N p_x (|\phi_x\rangle\langle\phi_x|)^{\otimes s} = \int (|\phi\rangle\langle\phi|)^{\otimes s} d\phi \quad (4)$$

holds for any $s \leq t$, where the integral is over the Haar measure.

We recall some results about quantum t -designs that will be useful in the following.

Lemma 3. *The integral over Haar measure in Eq. (4) is given by*

$$\int (|\phi\rangle\langle\phi|)^{\otimes s} d\phi = \frac{1}{M} P_{\text{sym}}, \quad (5)$$

where P_{sym} is the projector over the symmetric subspace and $M = \binom{s+d-1}{s}$ is its norm.

Proof. See Ref. [31]. \square

A t -design is called uniformly distributed (or unweighted) if $p_x = 1/N$ for all x . In this work we will focus on 2-designs. An ensemble $E = \{\rho_x\}$ of pure states is a 2-design ensemble if $\{p_x, |\phi_x\rangle\}$ is a 2-design, with $p_x := \text{Tr}[\rho_x]$ and $|\phi_x\rangle\langle\phi_x| := \rho_x / \text{Tr}[\rho_x]$. Notice that upon setting $s = 1$ in Eqs. (4) and (5), it follows that the average state of any 2-design ensemble is $\mathbb{1}/d$. This allows us to define 2-design POVMs as follows. A POVM $P = \{\Pi_y\}$ with rank-one elements is a 2-design POVM if $\{q_y, |\pi_y\rangle\}$ is a 2-design, with $q_y := \text{Tr}[\Pi_y]/d$ and $|\pi_y\rangle\langle\pi_y| := \Pi_y / \text{Tr}[\Pi_y]$.

Noticeable examples of uniformly-distributed 2-designs are symmetric informationally complete (SIC) sets [32], for which $N = d^2$, and $d+1$ mutually unbiased bases (MUBs) [34], for which $N = d(d+1)$.

Definition 4 (SIC). *A d -dimensional SIC set $\{p_x, |\phi_x\rangle\}_{x=1}^{d^2}$ is a uniform probability distribution $p_x = 1/d^2$ over normalized pure states $|\phi_x\rangle$ such that*

$$|\langle\phi_x|\phi_y\rangle|^2 = \frac{d\delta_{x,y} + 1}{d+1}. \quad (6)$$

Definition 5 (MUB). *A d -dimensional $(d+1)$ -MUB $\{p_{b,x}, |\phi_{b,x}\rangle\}_{b=1, x=1}^{d+1, d}$ is a uniform probability distribution $p_{b,x} = 1/(d(d+1))$ over normalized pure states $|\phi_{b,x}\rangle$ such that*

$$|\langle\phi_{b,x}|\phi_{b',x'}\rangle|^2 = \delta_{b,b'}\delta_{x,x'} + \frac{1}{d}(1 - \delta_{b,b'}). \quad (7)$$

III. ENTROPIC BOUNDS FOR 2-DESIGNS

In previous literature, entropic bounds for SICs and MUBs were discussed [44]. We generalize those results by providing bounds for arbitrary uniformly-distributed 2-designs.

Theorem 1. *The Shannon entropy $H(E, \Pi)$ of any 2-design ensemble $E = \{\rho_x\}_{x=1}^N$ uniformly distributed (namely, $\text{Tr}[\rho_x] = 1/N$ for all x) with respect to effect Π is bounded as follows:*

$$H(E, \Pi) \geq \log \left(\frac{N(d+1)}{d} \frac{\text{Tr}[\Pi]^2}{\text{Tr}[\Pi]^2 + \text{Tr}[\Pi^2]} \right). \quad (8)$$

Proof. Let $|\phi_x\rangle\langle\phi_x| := N\rho_x$. By setting $s = 2$ in Eqs. (4) and (5) it follows that

$$\sum_x \frac{1}{N} (|\phi_x\rangle\langle\phi_x|)^{\otimes 2} = \frac{\mathbb{1} + S}{d(d+1)},$$

where we used the fact that the projector on the symmetric subspace of $\mathcal{H}^{\otimes 2}$ is $P_{\text{sym}} = \frac{1}{2}(\mathbb{1} + S)$ and S is the swap operator.

Multiplying both sides by $\frac{d^2}{N} \frac{\Pi^{\otimes 2}}{\text{Tr}[\Pi]^2}$ and taking the trace we get

$$\sum_x \frac{d^2}{N^2} \frac{(\langle\phi_x|\Pi|\phi_x\rangle)^2}{\text{Tr}[\Pi]^2} = \frac{d}{N(d+1)} \frac{\text{Tr}[\Pi]^2 + \text{Tr}[\Pi^2]}{\text{Tr}[\Pi]^2}, \quad (9)$$

where we used the fact that $\text{Tr}[\Pi^{\otimes 2}S] = \text{Tr}[\Pi^2]$ for any effect Π .

Since the probability of state ρ_x given effect Π is given by

$$p_{x|\Pi} = \frac{d}{N} \frac{\langle\phi_x|\Pi|\phi_x\rangle}{\text{Tr}[\Pi]},$$

the negative logarithm of the left-hand side of Eq. (9) can be upper bounded by means of Jensen's inequality as follows:

$$-\log \sum_x p_{x|\Pi}^2 \leq -\sum_x p_{x|\Pi} \log p_{x|\Pi}.$$

The right-hand side is the Shannon entropy $H(E, \Pi)$ of ensemble E with respect to effect Π , so the statement follows. \square

Theorem 2. *The Shannon entropy $H(P, \rho)$ of any 2-design POVM $P = \{\Pi_y\}_{y=1}^N$ uniformly distributed (namely, $\text{Tr}[\Pi_y] = d/N$ for all y) with respect to state ρ is bounded as follows:*

$$H(P, \rho) \geq \log \left(\frac{N(d+1)}{d} \frac{\text{Tr}[\rho]^2}{\text{Tr}[\rho]^2 + \text{Tr}[\rho^2]} \right). \quad (10)$$

Proof. Let $|\pi_y\rangle\langle\pi_y| := N/d\Pi_y$. By setting $s = 2$ in Eqs. (4) and (5) it follows that

$$\sum_y \frac{1}{N} (|\pi_y\rangle\langle\pi_y|)^{\otimes 2} = \frac{\mathbb{1} + S}{d(d+1)},$$

where we used the fact that the projector on the symmetric subspace of $\mathcal{H}^{\otimes 2}$ is $P_{\text{sym}} = \frac{1}{2}(\mathbb{1} + S)$ and S is the swap operator.

Multiplying both sides by $\frac{d^2}{N} \frac{\rho^{\otimes 2}}{\text{Tr}[\rho]^2}$ and taking the trace we get

$$\sum_y \frac{d^2}{N^2} \frac{(\langle\pi_y|\rho|\pi_y\rangle)^2}{\text{Tr}[\rho]^2} = \frac{d}{N(d+1)} \frac{\text{Tr}[\rho]^2 + \text{Tr}[\rho^2]}{\text{Tr}[\rho]^2}, \quad (11)$$

where we used the fact that $\text{Tr}[\rho^{\otimes 2}S] = \text{Tr}[\rho^2]$ for any state ρ .

Since the probability of outcome Π_y given state ρ is given by

$$q_{y|\rho} = \frac{q}{N} \frac{\langle\pi_y|\rho|\pi_y\rangle}{\text{Tr}[\rho]},$$

the negative logarithm of the left-hand side of Eq. (11) can be upper bounded by means of Jensen's inequality as follows:

$$-\log \sum_y q_{y|\rho}^2 \leq -\sum_y q_{y|\rho} \log q_{y|\rho}.$$

The right-hand side is the Shannon entropy $H(P, \rho)$ of POVM P with respect to state ρ , so the statement follows. \square

By direct inspection it follows that state- and effect-dependent lower bounds in Eqs. (8) and (10) are independent of the norms of Π and ρ , so without loss of generality we can set $\text{Tr}[\rho] = \text{Tr}[\Pi] = 1$. Furthermore, those bounds can be made state- and effect-independent by minimizing the right hand side of Eqs. (8) and (10) over Π and ρ , respectively, with minimum achieved when Π and ρ are rank-one (namely, $\text{Tr}[\rho^2] = \text{Tr}[\Pi^2] = 1$).

IV. ACCESSIBLE INFORMATION AND INFORMATIONAL POWER OF 2-DESIGNS

In previous literature, the accessible information and the informational power of SICs were derived for dimension 2 [24, 25, 28] and 3 [29, 30], and tight bounds were provided for any dimension [29]. Bounds are also known for maximal sets of MUBs [1, 7]. In this section we generalize those results by providing bounds for 2-designs in any dimension.

Upper bounds on the accessible information and informational power of uniformly-distributed 2-designs can be derived from Theorems 1 and 2. However, in order to bound the accessible information of 2-designs in Theorem 3 we use an alternative derivation which holds for arbitrary (not necessarily uniformly-distributed) 2-design ensembles.

Theorem 3. *The accessible information $A(E)$ of any d -dimensional 2-design ensemble $E = \{\rho_x\}$ (not necessarily uniformly-distributed) is bounded as follows:*

$$A(E) \leq \log \frac{2d}{d+1}. \quad (12)$$

Proof. Let $p_x := \text{Tr}[\rho_x]$ and $|\phi_x\rangle\langle\phi_x| := \rho_x / \text{Tr}[\rho_x]$. By setting $s = 2$ in Eqs. (4) and (5) it follows that

$$\sum_x p_x (|\phi_x\rangle\langle\phi_x|)^{\otimes 2} = \frac{\mathbb{1} + S}{d(d+1)},$$

where we used the fact that the projector on the symmetric subspace of $\mathcal{H}^{\otimes 2}$ is $P_{\text{sym}} = \frac{1}{2}(\mathbb{1} + S)$ and S is the swap operator.

By Davies' theorem [22] it suffices to optimize over POVMs with rank-one elements. Let $P = \{\Pi_y\}$ be such a POVM and let $q_y := \text{Tr}[\Pi_y]/d$ and $|\pi_y\rangle\langle\pi_y| := \Pi_y / \text{Tr}[\Pi_y]$. Multiplying both sides by $d^2 \sum_y q_y (|\pi_y\rangle\langle\pi_y|)^{\otimes 2}$ and taking the trace we get

$$\sum_{x,y} p_x q_y d^2 |\langle\phi_x|\pi_y\rangle|^4 = \frac{2d}{d+1} \quad (13)$$

where we used the fact that $\text{Tr}[\Pi^{\otimes 2}S] = \text{Tr}[\Pi^2]$ for any effect Π .

Since the joint probability of state ρ_x and outcome Π_y is $p_{x,y} = p_x q_y d |\langle\phi_x|\pi_y\rangle|^2$, and its marginals are p_x and q_y (we recall that $\sum_x p_x |\phi_x\rangle\langle\phi_x| = \mathbb{1}/d$), the logarithm of the left-hand side of Eq. (13) can be lower bounded by means of Jensen's inequality as follows:

$$\sum_{x,y} p_{x,y} \log \frac{p_{x,y}}{p_x q_y} \leq \log \left(\sum_{x,y} p_{x,y} \frac{p_{x,y}}{p_x q_y} \right).$$

The left-hand side is the mutual information $I(E, P)$ between ensemble E and POVM P , namely

$$I(E, P) := \sum_{x,y} p_{x,y} \log \frac{p_{x,y}}{p_x q_y} \leq \log \frac{2d}{d+1}.$$

Since $A(E) := \sup_P I(E, P)$, the statement follows. \square

Theorem 4. *The informational power $W(P)$ of any 2-design POVM $P = \{\Pi_y\}$ uniformly distributed (namely, $\text{Tr}[\Pi_y] = d/N$ for all y) is bounded as follows:*

$$W(P) \leq \log \frac{2d}{d+1}. \quad (14)$$

Proof. Let $|\pi_y\rangle\langle\pi_y| := N/d\Pi_y$. By a Davies-like theorem [24] it suffices to optimize over ensembles of pure states. Let $E = \{\rho_x\}$ be such an ensemble and let $p_x := \text{Tr}[\rho_x]$ and $|\phi_x\rangle\langle\phi_x| := \rho_x / \text{Tr}[\rho_x]$. The joint probability of outcome Π_y given state ρ_x is then $p_{x,y} = p_x d/N |\langle\phi_x|\pi_y\rangle|^2$.

Let X, Y be random variables with X distributed according to p_x and Y such that $p(X = x, Y = y) = p_{x,y}$. Then one has

$$W(P) \geq I(E, P) = H(Y) - \sum_x H(Y|X = x)$$

One can trivially upper bound $H(Y)$ as $H(Y) \leq \log N$. Due to the state-independent version of Theorem 2, we have that $H(Y|X = x) \geq \log \frac{N(d+1)}{2d}$, from which the statement follows. \square

V. THE CASE OF SICS AND $(d+1)$ -MUBS

Almost forty years ago it was conjectured [22], and very recently proved [24, 29], that the accessible information and the informational power of 2-dimensional SIC ensembles and POVMs (tetrahedral configuration) is given by $\log 4/3$, with optimality achieved by the antipodal tetrahedral configuration. Very recently, the accessible information and the informational power $W(P)$ of 3-dimensional SIC ensembles and POVMs were proven [29, 30] to be given by $\log \frac{3}{2}$, with optimality achieved by an orthonormal configuration. We notice that these results follow as corollaries from Theorems 3 and 4.

Very recently, it was also proven [28] that the accessible information and the informational power of 2-dimensional 3-MUB ensembles and POVMs is given by $1/3$, with optimality achieved by a 3-MUB

configuration. In this Section we extend those results by deriving the accessible information and informational power of 3-dimensional 4-MUB ensembles and POVMs.

Corollary 1. *The accessible information $A(E)$ of any 3-dimensional 4-MUB ensemble E and the informational power $W(P)$ of any 3-dimensional 4-MUB POVM P is given by*

$$A(E) = W(P) = \log \frac{3}{2}. \quad (15)$$

The POVM attaining $A(E)$ is a SIC POVM and the ensemble attaining $W(P)$ is a SIC ensemble.

Proof. The 3-dimensional 4-MUB ensemble E or POVM P is unique [35] up to unitary transformations and permutations of elements. For some fixed orthonormal basis and up to a normalization, the coefficients of the vectors of E and P are given by the columns of the following matrix

$$\frac{1}{\sqrt{3}} \begin{bmatrix} \sqrt{3} & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \sqrt{3} & 0 & 1 & \omega & \omega^2 & \omega & \omega^2 & 1 & \omega^2 & \omega & 1 \\ 0 & 0 & \sqrt{3} & 1 & \omega^2 & \omega & \omega & 1 & \omega^2 & \omega^2 & 1 & \omega \end{bmatrix}$$

where $\omega = e^{i2\pi/3}$.

Denote with Q and F , respectively, the POVM and ensemble whose vectors are given, up to a normalization, by the columns of the following matrix

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & -1 & \xi & \xi^* \\ -1 & \xi & \xi^* & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & \xi & \xi^* & 0 & 0 & 0 \end{bmatrix}$$

where $\xi = e^{i\pi/3}$. It is immediate to verify that Q and F are a SIC POVM and ensemble, respectively.

By direct inspection it follows that $I(E, Q) = I(F, P) = \log 3/2$. Since by Definitions 1 and 2 we have $I(E, Q) \leq A(E)$ and $I(F, P) \leq W(P)$, and by Theorems 3 and 4 we have that $A(E), W(P) \leq \log 3/2$, the statement follows. \square

We now compare the optimal strategies attaining the accessible information and the informational power, with the so-called pretty-good strategies [45–48]. Given a d -dimensional 2-design ensemble $E = \{\rho_x\}$, its pretty-good POVM is $P = \{\Pi_x\}$ with $\Pi_x = d\rho_x$; analogously, given a d -dimensional 2-design POVM $P = \{\Pi_y\}$, its pretty-good ensemble is $E = \{\rho_y\}$ with $\rho_y = \Pi_y/d$.

For SIC ensembles and POVMs the mutual information given by the pretty-good strategy is

$$I(E, dE) = I(P/d, P) = \log d - \frac{d-1}{d} \log(d+1). \quad (16)$$

The right-hand side of Eq. (16) is smaller than the lower bound in Eq. (2) for any d . Then the pretty-good strategy for SIC ensembles and POVMs is suboptimal for any d .

For $(d+1)$ -MUB ensembles and POVMs the mutual information given by the pretty-good strategy is

$$I(E, dE) = I(P/d, P) = \frac{\log d}{d+1}. \quad (17)$$

The right-hand side of Eq. (17) coincides with the optimal value $1/3$ for $d = 2$. However, it is smaller than the value $\log 3/2$ provided by Corollary 1 for $d = 3$, and it is smaller than the lower bound in Eq. (2) for any $d \geq 4$. Then the pretty-good strategy for $(d+1)$ -MUB ensembles and POVMs is optimal for $d = 2$ and suboptimal for $d \geq 3$.

We report the results of this Section in Fig. 1.

VI. ARBITRARY-RANK SICs AND $(d+1)$ -MUBS

Symmetric informationally complete sets and mutually unbiased bases were generalized [49, 50] to the case of arbitrary-rank states and elements in the following way.

Definition 6 (Arbitrary-rank SIC set). *A d -dimensional arbitrary-rank SIC set $\{p_x, \rho_x\}_{x=1}^{d^2}$ is a uniform probability distribution $p_x = 1/d^2$ over mixed states ρ_x such that*

$$\text{Tr}[\rho_x \rho_{x'}] = \delta_{x,x'} d^2 a + (1 - \delta_{x,x'}) \frac{d(1 - da)}{d^2 - 1}. \quad (18)$$

for some $1/d^3 \leq a \leq 1/d^2$ and $\sum_x \rho_x = d\mathbb{1}$.

Notice that the rank-one case is recovered for $a = 1/d^2$, while for $a = 1/d^3$ one has a set of maximally mixed operators. An ensemble $E = \{\sigma_x\}$ is an *arbitrary-rank SIC ensemble* if $\{p_x, \rho_x\}$ is an arbitrary-rank SIC set, with $p_x := \text{Tr}[\sigma_x]$ and $\rho_x := \sigma_x / \text{Tr}[\sigma_x]$. A POVM $P = \{\Pi_y\}$ is an *arbitrary-rank SIC POVM* if $\{q_y, \rho_y\}$ is an arbitrary-rank SIC set, with $q_y := \text{Tr}[\Pi_y]/d$ and $\rho_y := \Pi_y / \text{Tr}[\Pi_y]$.

Definition 7 (Arbitrary-rank $(d+1)$ -MUB set). *A d -dimensional arbitrary-rank $(d+1)$ -MUB set $\{p_{b,x}, \rho_{b,x}\}_{b=1,\dots,d+1, x=1,\dots,d}$ is a uniform probability distribution $p_x = 1/d(d+1)$ over mixed states $\rho_{b,x}$ such that*

$$\begin{aligned} & \text{Tr}[\rho_{b,x} \rho_{b',x'}] \\ &= \delta_{b,b'} \delta_{x,x'} k + \delta_{b,b'} (1 - \delta_{x,x'}) \frac{1-k}{d-1} + \frac{1 - \delta_{b,b'}}{d}. \end{aligned} \quad (19)$$

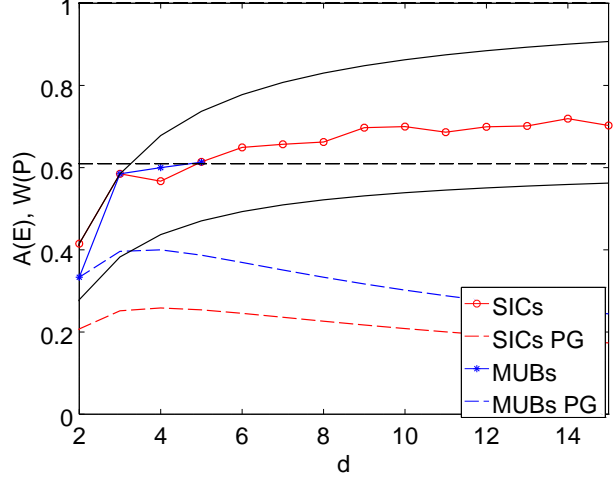


FIG. 1. (Color online) Upper and lower bounds [thick (black) continuous lines] and their asymptotes [horizontal (black) dashed lines] on accessible information $A(E)$ and informational power $W(P)$ of any 2-design ensemble E and uniformly-distributed 2-design POVM P , as a function of the dimension d , as given by Theorems 3 and 4. Accessible information and informational power of SIC ensembles and POVMs (red continuous line with circles), and corresponding pretty-good (PG) strategy [lower (red) dashed line] as in Eq. (16). Accessible information and informational power of $(d+1)$ -MUB ensembles and POVMs (blue continuous line with asterisks), and corresponding pretty-good (PG) strategy [upper (blue) dashed line] as in Eq. (17). For red and blue continuous lines (with circles and asterisks, respectively), values are analytically derived for $d = 2, 3$ (see Corollary 1), and numerically derived for $d \geq 4$. Numerical optimization was performed over SICs (up to dimension 15) and $(d+1)$ -MUBs (up to dimension 5, no example is known in dimension 6) as provided in Refs. [33, 35].

for some $1/d \leq k \leq 1$ and $\sum_{b,x} \rho_{b,x} = (d+1)\mathbb{1}$.

Notice that the rank-one case is recovered for $k = 1$, while for $k = 1/d$ one has a set of maximally mixed operators. An ensemble $E = \{\sigma_{b,x}\}$ is an *arbitrary-rank $(d+1)$ -MUB ensemble* if $\{p_{b,x}, \rho_{b,x}\}$ is an arbitrary-rank $(d+1)$ -MUB set, with $p_{b,x} := \text{Tr}[\sigma_{b,x}]$ and $\rho_{b,x} := \sigma_{b,x} / \text{Tr}[\sigma_{b,x}]$. A POVM $P = \{\Pi_{b,y}\}$ is an *arbitrary-rank MUB POVM* if $\{q_{b,y}, \rho_{b,y}\}$ is an arbitrary-rank $(d+1)$ -MUB set, with $q_{b,y} := \text{Tr}[\Pi_{b,y}]/d$ and $\rho_{b,y} := \Pi_{b,y} / \text{Tr}[\Pi_{b,y}]$.

Theorem 5. *The accessible information $A(E)$ of any arbitrary-rank SIC ensemble $E = \{\rho_x\}$ and the informational power $W(P)$ of any arbitrary-rank*

SIC POVM $P = \{\Pi_y\}$ are bounded as follows:

$$A(E), W(P) \leq \log \frac{d(d^2a + 1)}{d + 1}. \quad (20)$$

Proof. Let us first prove the statement for $W(P)$, then the statement for $A(E)$ will immediately follow from Lemmas 1 and 3.

By a Davies-like theorem [24] it suffices to optimize over ensembles of pure states. Let $F = \{\sigma_x\}$ be such an ensemble and let $p_x := \text{Tr}[\sigma_x]$ and $|\phi_x\rangle\langle\phi_x| := \sigma_x / \text{Tr}[\sigma_x]$. The joint probability of state σ_x and outcome Π_y is then $p_{x,y} = p_x \langle\phi_x|\Pi_y|\phi_x\rangle$.

Let X, Y be random variables with X distributed according to p_x and Y such that the joint probability of X and Y is $p_{x,y}$. Then one has

$$W(P) \geq I(E, P) = H(Y) - \sum_x p_x H(Y|X = x).$$

One can trivially upper bound $H(Y)$ as $H(Y) \leq \log d^2$. It was proven [51] that

$$H(Y|X = x) \geq -\log \left(\frac{ad^3 - ad^2 + d - 1}{d(d^2 - 1)} \right),$$

from which the statement follows. \square

Theorem 6. *The accessible information $A(E)$ of any generalized $(d + 1)$ -MUB ensemble $E = \{\rho_x\}$ and the informational power $W(P)$ of any generalized $(d + 1)$ -MUB POVM $P = \{\Pi_y\}$ are bounded as follows:*

$$A(E), W(P) \leq \log \frac{d(k + 1)}{d + 1}. \quad (21)$$

Proof. Let us first prove the statement for $W(P)$, then the statement for $A(E)$ will immediately follow from Lemmas 1 and 3.

By a Davies-like theorem [24] it suffices to optimize over ensembles of pure states. Let $F = \{\sigma_x\}$ be such an ensemble and let $p_x := \text{Tr}[\sigma_x]$ and $|\phi_x\rangle\langle\phi_x| := \sigma_x / \text{Tr}[\sigma_x]$. The joint probability of state σ_x and outcome Π_y is then $p_{x,y} = p_x \langle\phi_x|\Pi_y|\phi_x\rangle$.

Let X, Y be random variables with X distributed according to p_x and Y such that the joint probability of X and Y is $p_{x,y}$. Then one has

$$W(P) \geq I(E, P) = H(Y) - \sum_x p_x H(Y|X = x).$$

One can trivially upper bound $H(Y)$ as $H(Y) \leq \log(d(d + 1))$. It was proven [52] that

$$H(Y|X = x) \geq \log \frac{(d + 1)^2}{k + 1},$$

from which the statement follows. \square

Notice that bounds on the accessible information and informational power of rank-one SIC ensembles and POVMs [29] can be obtained as a corollary of Theorem 5 by setting $a = 1/d^2$; analogously, bounds for $(d + 1)$ -MUBs [1, 7] can be obtained as a corollary of Theorem 6 by setting $k = 1$. In the maximally mixed case, by setting $a = 1/d^3$ (resp., $k = 1/d$) in Theorem 5 (resp. Theorem 6), one has that accessible information and informational power vanish as expected.

VII. CONCLUSION AND OUTLOOK

We derived effect-dependent and effect-independent lower bounds on the entropy of the input distribution of 2-design ensembles; analogously, we derived state-dependent and state-independent lower bounds on the entropy of the output distribution of 2-design measurements. From these results, we derived upper bounds on the accessible information and the informational power of 2-design ensembles and measurements, as a function of the dimension of the system only. As a consequence, we showed that, perhaps surprisingly, the statistics generated by 2-designs, although optimal for testing of entropic uncertainty relations, quantum cryptography and tomography, never contains more than one bit of information. As particular cases, we provided the accessible information and informational power of SIC and MUB ensembles and POVMs (analytically for dimensions two and three, numerically otherwise). Finally, we extended our results to generalizations of SICs and MUBs with arbitrary rank.

We conclude by presenting a few relevant open problems. Analytically characterizing the accessible information and the informational power of SIC ensembles and POVMs in dimension larger than 3 seems a hard task, as suggested by the irregular behavior of the corresponding line in Fig. 1. However, preliminary results seem to suggest that the same task for $(d + 1)$ -MUB ensembles and POVMs could be feasible. Indeed, consider the unique [35] (up to unitary transformations and permutation of elements) 4-dimensional $(d + 1)$ -MUB ensemble E and POVM P , whose coefficients with respect to some fixed orthonormal basis are given (up to a normal-

ization) by the columns of the following matrices

$$\frac{1}{2} \begin{bmatrix} 2 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 0 & 1 & 1 & -1 & -1 & -1 & -1 \\ 0 & 0 & 2 & 0 & 1 & -1 & -1 & 1 & -i & i \\ 0 & 0 & 0 & 2 & 1 & -1 & 1 & -1 & -i & i \end{bmatrix},$$

$$\frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -i & -i & i & i & -i & -i & i & i \\ i & -i & -i & i & i & -i & -1 & 1 & -1 & 1 \\ -i & i & -1 & 1 & -1 & 1 & -i & i & i & -i \end{bmatrix}.$$

The orthonormal POVM Q and ensemble F given by

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{i}{\sqrt{2}} & -\frac{i}{2} & 0 & -\frac{i}{2} \\ 0 & -\frac{i}{2} & \frac{i}{\sqrt{2}} & \frac{i}{2} \\ 0 & \frac{1}{2} & \frac{1}{\sqrt{2}} & -\frac{1}{2} \end{bmatrix}$$

are such that $I(E, Q) = I(F, P) = 3/5$, and we conjecture that this value is optimal, namely $A(E) = W(P) = 3/5$.

Another relevant open problem is whether there exists a maximally informative 2-design, namely a 2-design saturating the upper bound in Theorems 3 and 4 for any dimension d . We showed that the

answer is on the affirmative for $d = 2$, where SIC ensembles and POVMs are optimal, and for $d = 3$, where both SIC and $(d + 1)$ -MUB ensembles and POVMs are optimal. However, numerical results presented in Fig. 1 seem to suggest that, for $d \geq 4$, nor SICs nor $(d + 1)$ -MUBs are maximally informative 2-designs.

Finally, a very interesting open question is how to generalize arbitrary quantum 2-designs to the arbitrary-rank case, in the same spirit of the generalizations for SICs and MUBs previously discussed [49, 50], and how to quantify their accessible information and informational power. We believe that these tantalizing open problems well deserve future investigation.

ACKNOWLEDGMENTS

The author is grateful to Francesco Buscemi, Chris Fuchs, Massimiliano F. Sacchi, Wojciech Słomczyński, Anna Szymusiak, and Vlatko Vedral for very useful discussions, comments, and suggestions. This work was supported by the Ministry of Education and the Ministry of Manpower (Singapore).

-
- [1] J. Sánchez-Ruiz, Phys. Lett. A **201**, 125 (1995).
 - [2] M. A. Ballester and S. Wehner, Phys. Rev. A **75**, 022319 (2007).
 - [3] S. Wehner and A. Winter, New J. Phys. **12**, 025009 (2010).
 - [4] I. Białynicki-Birula and L. Rudnicki, *Statistical Complexity: Applications in Electronic Structure*, Ed. K. D. Sen, (Springer, U.K., 2011), chapter 1.
 - [5] F. Buscemi, M. J. W. Hall, M. Ozawa, and M. M. Wilde, Phys. Rev. Lett. **112**, 050401 (2014).
 - [6] N. Brunner, *Device-Independent Quantum Information Processing*, in Proceedings of the Quantum Information and Measurement Conference (2014).
 - [7] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **92**, 067902 (2004).
 - [8] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing 175, 8 (1984).
 - [9] G. Mauro D'Ariano, M. De Laurentis, M. G. A. Paris, A. Porzio, S. Solimeno, J. Opt. B: Quantum Semiclass. Opt. **4**, 127 (2002).
 - [10] M. Dall'Arno, Scientifica Acta **5**, 22 (2011).
 - [11] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Phys. Rev. Lett. **105**, 230501 (2010).
 - [12] M. Dall'Arno, E. Passaro, R. Gallego, A. Acín, Phys. Rev. A **86**, 042312 (2012).
 - [13] F. Buscemi, G. Gour, and J. S. Kim, Phys. Rev. A **80**, 012324 (2009).
 - [14] F. Buscemi, New J. Phys. **12**, 123002 (2009).
 - [15] M. Dall'Arno, G. M. D'Ariano, and M. F. Sacchi, Phys. Rev. A **82**, 042315 (2010).
 - [16] F. Buscemi, Phys. Rev. A **77**, 012309 (2008).
 - [17] G. Chiribella, M. Dall'Arno, G. M. D'Ariano, C. Macchiavello, and P. Perinotti, Phys. Rev. A **83**, 052305 (2011).
 - [18] D. S. Lebedev, L. B. Levitin, Information and Control **9**, 1 (1966).
 - [19] A. S. Holevo, J. Multivariate Anal. **3**, 337 (1973).
 - [20] V. P. Belavkin, Stochastics **1**, 315 (1975).
 - [21] V. P. Belavkin, Radio Engineering and Electronic Physics **20**, 39 (1975).
 - [22] E. B. Davies, IEEE Trans. Inf. Theory **24**, 596 (1978).
 - [23] R. Jozsa, D. Robb, and W. K. Wootters, Phys. Rev. A **49**, 668 (1994).
 - [24] M. Dall'Arno, G. M. D'Ariano, and M. F. Sacchi, Phys. Rev. A **83**, 062304 (2011).

- [25] O. Oreshkov, J. Calsamiglia, R. Muñoz-Tapia, and E. Bagan, *New J. Phys.* **13**, 073032 (2011).
- [26] A. S. Holevo, *Problems of Information Transmission* **48**, 1 (2012).
- [27] A. S. Holevo, *Phys. Scr.* **2013**, 014034 (2013).
- [28] W. Słomczyński and A. Szymusiak, arXiv:1402.0375.
- [29] M. Dall’Arno, F. Buscemi, and M. Ozawa, *J. Phys. A: Math. Theor.* **47**, 235302 (2014).
- [30] A. Szymusiak, *J. Phys. A: Math. Theor.* **47**, 445301 (2014).
- [31] A. Ambainis and J. Emerson, “*Quantum t-designs: t-wise independence in the quantum world*,” in *Proceedings of the Twenty-Second Annual IEEE Conference on Computational Complexity*, 129 (2007).
- [32] G. Zauner, *Quantendesigns Grundzuge einer nichtkommutativen Designtheorie*. Dissertation, Universitat Wien, 1999.
- [33] A. J. Scott and M. Grassl, *Journal of Mathematical Physics* **51**, 042203 (2010).
- [34] A. Klappenecker and M. Roetteler, *Proceedings 2005 IEEE International Symposium on Information Theory (ISIT 2005)*, 1740 (2005).
- [35] S. Brierley, S. Weigert, and I. Bengtsson, *Quantum Info. & Comp.* **10**, 0803 (2010).
- [36] C. A. Fuchs and M. Sasaki, *Quantum Inf. & Comput.* **3**, 377 (2003).
- [37] C. A. Fuchs, *Quantum Inf. & Comput.* **4**, 467 (2004).
- [38] C. A. Fuchs and R. Schack, *Rev. Mod. Phys.* **85**, 1693 (2013).
- [39] C. A. Fuchs and R. Schack, *Foundations of Physics* **41**, 345 (2011).
- [40] D. M. Appleby, Å. Ericsson, and C. A. Fuchs, *Foundations of Physics* **41**, 564 (2011).
- [41] C. Fuchs, arXiv:1207.2141
- [42] I. L. Chuang and M. A. Nielsen, *Quantum Information and Communication* (Cambridge, Cambridge University Press, 2000).
- [43] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Hoboken, Wiley-Interscience, 2006).
- [44] A. E. Rastegin, *Eur. Phys. J. D* **67**, 269 (2013).
- [45] P. Hausladen and W. K. Wootters, *J. Mod. Opt.* **41**, 2385 (1994).
- [46] M. J. W. Hall, *Phys. Rev. A* **55**, 100 (1997).
- [47] F. Buscemi, *Phys. Rev. Lett.* **99**, 180501 (2007).
- [48] F. Buscemi and M. Horodecki, *OSID* **16**, 29 (2009).
- [49] A. Kalev and G. Gour, *J. Phys. A: Math. Theor.* **47**, 335302 (2014).
- [50] A. Kalev and G. Gour, *New Journal of Physics* **16**, 053038 (2014).
- [51] A. E. Rastegin, *Physica Scripta* **89**, 085101 (2014).
- [52] B. Chen, and S.-H. Fei, arXiv:1407.6816.